

**CLAIMS:**

What is claimed is:

1. A method in a digital camera for verifying that a particular digital visual image was produced by said digital camera, said method comprising the steps of:

storing a visual image in a digital format in said camera;

generating a digital signature for said image utilizing said camera only in response to said storage of said image in said camera, said digital signature associating said stored image with said camera;

storing said digital signature only in said camera, said signature being stored separately from said image in said camera, said digital signature capable of being utilized only within said camera by only said camera, wherein said signature is inaccessible to devices other than said camera; and

subsequently authenticating said particular digital visual image as being produced by said digital camera utilizing said digital signature stored in said digital camera, wherein only said digital camera is capable of authenticating said particular digital visual image.

1       2.    The method according to claim 1, further comprising the  
2       steps of:

3               storing said visual image in a file within said camera,  
4       said file being designated by a filename; and

5               storing said signature in said camera with said  
6       filename.

1       3.    The method according to claim 1, further comprising the  
2       steps of:

3               establishing a hardware master key pair for said  
4       digital camera, said hardware master key pair including a  
5       master private key and a master public key, said hardware  
6       master key pair being associated with said digital camera so  
7       that said master private key is known to only said digital  
8       camera;

9               establishing a signature device having an encryption  
10      engine and a protected storage device, said protected  
11      storage device being accessible only through said encryption  
12      engine; and

13              storing said hardware master key pair in said protected  
14      storage device.

1       4.    The method according to claim 3, wherein said step of  
2   generating a digital signature further comprises the steps  
3   of:

4            hashing said stored image to produce an original image  
5   digest;

6            signing said first digest utilizing said master private  
7   key; and

8            storing said signed original image digest as said  
9   signature.

1       5.    The method according to claim 4, wherein said step of  
2   authenticating said visual image further comprises the steps  
3   of:

4            retrieving an image to authenticate;

5            retrieving a signature for said image which is to be  
6   authenticated;

7            hashing said image which is to be authenticated to  
8   produce a first digest;

9            decrypting said retrieved signature to retrieve a  
10   second digest;

11           comparing said first digest to said second digest;

12           determining that said image has been altered in  
13           response to a determination that said first and second  
14           digests do not match; and

15           determining that said image has not been altered in  
16           response to a determination that said first and second  
17           digests match.

1           6.   The method according to claim 1, wherein said step of  
2           generating a digital signature further comprises the steps  
3           of:

4                hashing said stored image to produce an original image  
5                digest;

6                signing said first digest utilizing a master private  
7                key; and

8                storing said signed original image digest as said  
9                signature.

1           7.   The method according to claim 6, wherein said step of  
2           authenticating said visual image further comprises the steps  
3           of:

4                retrieving an image to authenticate;

5                retrieving a signature for said image which is to be  
6                authenticated;

7            hashing said image which is to be authenticated to  
8            produce a first digest;

9            decrypting said retrieved signature to retrieve a  
10           second digest;

11           comparing said first digest to said second digest;

12           determining that said image has been altered in  
13           response to a determination that said first and second  
14           digests do not match; and

15           determining that said image has not been altered in  
16           response to a determination that said first and second  
17           digests match.

1       8.    A digital camera for verifying that a particular  
2       digital visual image was produced by said digital camera,  
3       comprising:

4           memory means for storing a visual image in a digital  
5       format in said camera;

6           a signature device for generating a digital signature  
7       for said image utilizing said camera only in response to  
8       said storage of said image in said camera, said digital  
9       signature associating said stored image with said camera;

10          memory means for storing said digital signature only in  
11       said camera, said signature being stored separately from  
12       said image in said camera, said digital signature capable of  
13       being utilized only within said camera by only said camera,  
14       wherein said signature is inaccessible to devices other than  
15       said camera; and

16          means for subsequently authenticating said particular  
17       digital visual image as being produced by said digital  
18       camera utilizing said digital signature stored in said  
19       digital camera, wherein only said digital camera is capable  
20       of authenticating said particular digital visual image.

1 9. The digital camera according to claim 8, further  
2 comprising:

3 said memory means for storing said visual image in a  
4 file within said camera, said file being designated by a  
5 filename; and

6 said memory means for storing said signature in said  
7 camera with said filename.

1 10. The digital camera according to claim 8, further  
2 comprising:

3 said signature device including stored within it a  
4 hardware master key pair for said digital camera, said  
5 hardware master key pair including a master private key and  
6 a master public key, said hardware master key pair being  
7 associated with said digital camera so that said master  
8 private key is known to only said digital camera; and

9 said signature device having an encryption engine and a  
10 protected storage device, said protected storage device  
11 being accessible only through said encryption engine.

1 11. The digital camera according to claim 10, further  
2 comprising:

3 means for hashing said stored image to produce an  
4 original image digest;

5 means for signing said first digest utilizing said  
6 master private key; and

7 means for storing said signed original image digest as  
8 said signature.

1 12. The digital camera according to claim 11, further  
2 comprising:

3 means for retrieving an image to authenticate;

4 means for retrieving a signature for said image which  
5 is to be authenticated;

6 means for hashing said image which is to be  
7 authenticated to produce a first digest;

8 means for decrypting said retrieved signature to  
9 retrieve a second digest;

10 means for comparing said first digest to said second  
11 digest;

12 means for determining that said image has been altered  
13 in response to a determination that said first and second  
14 digests do not match; and

15 means for determining that said image has not been  
16 altered in response to a determination that said first and  
17 second digests match.



1 13. The digital camera according to claim 8, further  
2 comprising:

3 means for hashing said stored image to produce an  
4 original image digest;

5 means for signing said first digest utilizing a master  
6 private key; and

7 means for storing said signed original image digest as  
8 said signature.

1 14. The digital camera according to claim 13, further  
2 comprising:

3 means for retrieving an image to authenticate;

4 means for retrieving a signature for said image which  
5 is to be authenticated;

6 means for hashing said image which is to be  
7 authenticated to produce a first digest;

8 means for decrypting said retrieved signature to  
9 retrieve a second digest;

10 means for comparing said first digest to said second  
11 digest;

12 means for determining that said image has been altered  
13 in response to a determination that said first and second  
14 digests do not match; and

15 means for determining that said image has not been  
16 altered in response to a determination that said first and  
17 second digests match.

2025 RELEASE UNDER E.O. 14176